



Powered by  
**Faast**



## Pentesting persistente para dispositivos IoT

¿Qué pasaría si hackean nuestra empresa a través de dispositivos IoT? Webcams, impresoras, routers, TVs o teléfonos IP están conectados a la red corporativa, se intercomunican con el resto de sistemas y también con servidores externos, abriendo una nueva vía de ataque para los cibercriminales.

Este marco de inseguridad ha motivado a nuestro equipo experto en técnicas de hacking a desarrollar una nueva funcionalidad para Faast. Nuestra herramienta de pentesting persistente ahora también escanea tus sistemas descubriendo los dispositivos IoT conectados a la red, detectando cualquier error de configuración o fallo de seguridad que permita a un usuario no autorizado acceder a los datos de tu organización.

## La primera tecnología que permite detectar y analizar de forma persistente las nuevas vulnerabilidades de dispositivos IoT



### Innovación

Esta nueva funcionalidad ofrece el escaneo constante y recursivo de los dispositivos IoT de tu organización.



### Personalización

Adaptamos las estrategias de escaneo en base a la capacidad de respuesta de tu sistema.



### Visión Global

Aplica técnicas de atacantes reales ayudando a cubrir todas las fases de vida de una ciberamenaza.



### Inteligencia

Un planteamiento totalmente nuevo para la fortificación de la red y la infraestructura IoT.



### Equipo técnico

Equipo experto en técnicas de hacking que analiza y valida las vulnerabilidades detectadas.

## Faast en tu empresa

- Descubre los dispositivos IoT conectados a tu infraestructura, tanto los que conoces como los que no (Shadow IT/Shadow IoT).
- Detecta las principales vulnerabilidades presentes en ecosistemas IoT (web interface insegura, autenticación/autorización insuficiente, servicios de red inseguros, falta de cifrado en capa de transporte, credenciales conocidas, cross-site scripting, ataques de inyección).
- Descubre las vulnerabilidades de dispositivos conectados a tu empresa como televisores, centralitas de telefonía VoIP o sistemas de videoconferencias que pueden ser utilizadas como vía de ataque, circunvalando las medidas de seguridad perimetral implantadas.
- Gestiona las vulnerabilidades de tus activos IoT a través del portal online de Vamps.

## A quién va destinado

Nuestra tecnología Faast para dispositivos IoT está diseñada para:

- Investigadores y analistas que buscan nuevas soluciones de seguridad escalables a la heterogeneidad de las diferentes tecnologías de los dispositivos IoT.
- Empresas que prestan servicios de seguridad o de ciberinteligencia que necesitan cubrir este nuevo nicho de mercado.
- Departamentos IT para los cuales la gestión de dispositivos IoT se ha convertido en un auténtico quebradero de cabeza.